Amendments to the Claims

Claim 1 (currently amended): A method of improving intrusion detection in a computing network, comprising steps of:

defining a plurality of intrusion suspicion levels for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, defining a set of at least one conditions which describe the potential intrusion event;

associating one of the defined intrusion suspicion levels with each of the sets of conditions;

defining a plurality of sensitivity levels for filtering intrusion events when performing the intrusion detection processing; and

performing intrusion detection for a particular inbound communication received for the computing device, further comprising steps of:

determining whether any of the at least one sets of conditions are matched; and

if so, using a currently-applicable one of the defined sensitivity levels, in concert with the ~~defined~~ intrusion suspicion ~~levels~~ level associated with the matched conditions, to determine if [[a]] the particular inbound communication ~~destined for the computing device~~ should be treated as an intrusion event.

Claim 2 (canceled)

Claim 3 (currently amended): The method according to Claim [[2]] 1, wherein the determining step further comprises comparing current conditions in the computing device to ~~predetermined conditions which signal a potential intrusion~~ the conditions defined in at least one of the sets.

Claim 4 (currently amended): The method according to Claim 3, wherein the current conditions in the computing device comprise contents of the particular inbound communication.

Claim 5 (currently amended): The method according to Claim 4, wherein the current conditions in the computing device further comprise a protocol state of a protocol stack which processes the particular inbound communication.

Claim 6 (currently amended): The method according to Claim 1, further comprising the step of taking one or more defensive actions ~~when the using step determines~~ upon determining that the particular inbound communication should be treated as an intrusion event.

Claim 7 (original): The method according to Claim 6, wherein the defensive actions are determined by consulting intrusion detection policy information.

Claim 8 (currently amended): The method according to Claim [[6]] 7, wherein the intrusion detection policy information is stored in a network-accessible repository.

Claim 9 (currently amended): The method according to Claim 1, wherein the ~~using step further~~

~~comprises comparing the particular inbound communication to~~ defined at least one set of conditions represents one or more attack signatures.

Claim 10 (original): The method according to Claim 9, wherein at least one of the attack signatures is a class signature representing a class of attacks.

Claim 11 (currently amended): The method according to Claim [[9]] 1, wherein each of the at least one set of conditions is ~~attack signatures are~~ specified ~~as conditions~~ as a condition part in an intrusion detection [[rules]] rule, and wherein each of the intrusion detection rules further specifies at least one action ~~comprises one or more actions that are~~ to be taken upon determining ~~when the using step determines~~ that the particular inbound communication should be treated as an intrusion event.

Claim 12 (currently amended): The method according to Claim 1, wherein the performing [[using]] step operates in the computing device for which the particular inbound communication is destined.

Claim 13 (currently amended): The method according to Claim 12, wherein the performing [[using]] step operates within layer-specific intrusion detection logic executing in a protocol stack running on the computing device.

Claim 14 (currently amended): The method according to Claim 1, wherein the performing

[[using]] step operates in a network device which analyzes communications directed to the computing device for which the particular inbound communication is destined.

Claim 15 (currently amended): The method according to Claim 1, ~~further comprising steps of:~~

~~for each of a plurality of potential intrusion events, defining a set of one or more conditions which describe the potential intrusion event;~~

~~associating a sensitivity level with each of the sets of conditions; and~~

~~determining a suspicion level of the particular inbound communication;~~

~~wherein~~ the using step further comprises consulting a stored mapping between each of the defined sensitivity levels and each of the defined intrusion suspicion levels, using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched conditions, to determine if ~~determines that~~ the particular inbound communication should be treated as an intrusion event ~~when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions and the determined suspicion level maps to the sensitivity level associated with the selected set of conditions~~.

Claims 16 - 21 (canceled)

Claim 22 (currently amended): A system for improving intrusion detection in a computing network, comprising:

~~means for defining~~ a plurality of intrusion suspicion levels defined for use when performing intrusion detection processing on inbound communications destined for a computing

device on the computing network;

for each of a plurality of potential intrusion events, a defined set of at least one conditions which describe the potential intrusion event;

means for associating one of the defined intrusion suspicion levels with each of the defined sets of conditions;

a plurality of sensitivity levels defined for filtering intrusion events when performing the intrusion detection processing; and

means for performing intrusion detection for a particular inbound communication received for the computing device, further comprising:

means for determining whether any of the at least one defined sets of conditions are matched; and

if so, means for using a currently-applicable one of the defined sensitivity levels, in concert with the ~~defined~~ intrusion suspicion ~~levels~~ level associated with the matched conditions, to determine if [[a]] the particular inbound communication destined for the computing device should be treated as an intrusion event.

Claim 23 (canceled)

Claim 24 (currently amended): The system according to Claim [[23]] 22, wherein the means for determining further comprises means for comparing current conditions in the computing device ~~to predetermined conditions which signal a potential intrusion~~ the conditions defined in at least one of the sets.

Claim 25 (currently amended): The system according to Claim 22, further comprising means for taking one or more defensive actions ~~when the means for using determines~~ upon determining that the particular inbound communication should be treated as an intrusion event, wherein the defensive actions are determined by consulting intrusion detection policy information.

Claim 26 (currently amended): The system according to Claim 22, wherein each of ~~the means for using further comprises means for comparing the particular inbound communication to~~ at least one set of conditions is ~~one or more attack signatures, wherein the attack signatures are~~ specified as ~~conditions~~ a condition part in an intrusion detection ~~rules~~ rule, and wherein each of the intrusion detection rules further ~~comprises~~ specifies at least one action ~~one or more actions that are~~ to be taken upon determining ~~when the means for using determines~~ that the particular inbound communication should be treated as an intrusion event.

Claim 27 (currently amended): The system according to Claim 22, ~~further comprising:~~

~~for each of a plurality of potential intrusion events, means for defining a set of one or more conditions which describe the potential intrusion event;~~

~~means for associating a sensitivity level with each of the sets of conditions; and~~

~~means for determining a suspicion level of the particular inbound communication;~~

~~wherein~~ the means for using further comprises means for consulting a stored mapping between each of the defined sensitivity levels and each of the defined intrusion suspicion levels, using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion

level associated with the matched conditions, to determine if ~~determines that~~ the particular inbound communication should be treated as an intrusion event ~~when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions and the determined suspicion level maps to the sensitivity level associated with the selected set of conditions~~.

Claims 28 - 31 (canceled)

Claim 32 (currently amended): A computer program product for improving intrusion detection in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code ~~means for~~ defining a plurality of intrusion suspicion levels for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, computer-readable program code defining a set of at least one conditions which describe the potential intrusion event;

computer-readable program code associating one of the defined intrusion suspicion levels with each of the sets of conditions;

computer-readable program code defining a plurality of sensitivity levels for filtering intrusion events when performing the intrusion detection processing; and

computer-readable program code for performing intrusion detection for a particular inbound communication received for the computing device, further comprising:

computer-readable program code for determining whether any of the at least one sets of conditions are matched; and

if so, computer-readable program code [[means]] for using a currently-applicable one of the defined sensitivity levels, in concert with the ~~defined~~ intrusion suspicion ~~levels~~ level associated with the matched conditions, to determine if [[a]] the particular inbound communication ~~destined for the computing device~~ should be treated as an intrusion event.

Claim 33 (canceled)

Claim 34 (currently amended): The computer program product according to Claim [[33]] 32, wherein the computer-readable program code [[means]] for determining further comprises computer-readable program code [[means]] for comparing current conditions in the computing device to ~~predetermined conditions which signal a potential intrusion~~ the conditions defined in at least one of the sets, the current conditions in the computing device comprising contents of the particular inbound communication.

Claim 35 (currently amended): The computer program product according to Claim [[33]] 32, wherein the computer-readable program code [[means]] for determining further comprises computer-readable program code [[means]] for comparing current conditions in the computing device to ~~predetermined conditions which signal a potential intrusion~~ the conditions defined in at least one of the sets, the current conditions in the computing device comprising contents of the particular inbound communication and a protocol state of a protocol stack which processes the

particular inbound communication.

Claim 36 (currently amended): The computer program product according to Claim 32, further comprising computer-readable program code [[means]] for taking one or more defensive actions upon determining ~~when the computer-readable program code means for using determines~~ that the particular inbound communication should be treated as an intrusion event, wherein the defensive actions are determined by consulting intrusion detection policy information stored in a policy repository.

Claim 37 (currently amended): The computer program product according to Claim [[1]] 32, wherein the ~~computer-readable program code means for using further comprises computer-readable program code means for comparing the particular inbound communication to~~ defined at least one set of conditions represents one or more attack signatures, wherein at least one of the attack signatures is a class signature representing a class of attacks.

Claim 38 (currently amended): The computer program product according to Claim 32, wherein the computer-readable program code [[means]] for [[using]] performing operates in the computing device for which the particular inbound communication is destined.

Claim 39 (currently amended): The computer program product according to Claim 32, wherein the computer-readable program code [[means]] for [[using]] performing operates in a network device which analyzes communications directed to the computing device for which the particular

inbound communication is destined.

Claim 40 (currently amended): The computer program product according to Claim 32, ~~further comprising:~~

~~computer-readable program code means for specifying, for each of a plurality of potential intrusion events, a set of one or more conditions which describe the potential intrusion event;~~

~~computer-readable program code means for associating a sensitivity level with each of the sets of conditions; and~~

~~computer-readable program code means for determining a suspicion level of the particular inbound communication;~~

~~wherein~~ the computer-readable program code [[means]] for using further comprises computer-readable code for consulting a stored mapping between each of the defined sensitivity levels and each of the defined intrusion suspicion levels, using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched conditions, to determine if ~~determines that~~ the particular inbound communication should be treated as an intrusion event ~~when conditions pertaining to the particular inbound communication match a selected one of the sets of conditions and the determined suspicion level maps to the sensitivity level associated with the selected set of conditions~~.

Claims 41 - 44 (canceled)

Claim 45 (new): The method according to Claim 6, wherein the defensive actions are specified

as actions in a rule in which the matched conditions are specified.

Claim 46 (new): The method according to Claim 6, wherein at least one of the defensive actions comprises discarding the particular inbound communication.

Claim 47 (new): The method according to Claim 6, wherein at least one of the defensive actions comprises limiting at least one of resources or traffic associated with a connection on which the particular inbound communication is received.

Claim 48 (new): The method according to Claim 6, wherein at least one of the defensive actions comprises dynamically dropping a deny filter into the computing network to shun subsequent traffic.

Claim 49 (new): The method according to Claim 6, wherein at least one of the defensive actions comprises reporting the intrusion event to one or more entities.

Claim 50 (new): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises sending an alert to a management component external from the computing device for which the particular inbound communication is destined.

Claim 51 (new): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises writing at least one event record to at least one of a system

log and a console.

Claim 52 (new): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises recording inbound communications associated with the intrusion event in at least one of a trace or other repository.

Claim 53 (new): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises writing statistics records on normal behavior to establish baselines as to what constitutes abnormal behavior for the inbound communications.

Claim 54 (new): The method according to Claim 1, wherein at least one of the defined sets of conditions specifies a current system state of the computing device.

Claim 55 (new): The method according to Claim 1, wherein at least one of the defined sets of conditions specifies at least one threshold reached at the computing device.

Claim 56 (new): The method according to Claim 1, wherein at least one of the defined sets of conditions specifies at least one state transition to be caused, at the computing device, upon receiving the particular inbound communication.

Claim 57 (new): The method according to Claim 1, wherein the currently-applicable sensitivity level is specified, for the computing device, by a systems administrator.

Claim 58 (new): The method according to Claim 1, wherein the currently-applicable sensitivity level is specified, for the computing device, by configuration data in a stored repository.